

ABSTRACT OF THE DISCLOSURE

The inventive method enables the signing and/or encrypting of a message to be transmitted from a sending party to a receiving party over a telecommunication network with the ability to ascertain from the message the identity of the sender and the integrity of the message contents. The message for transmission is divided into at least a header section, to which a sender identification is added, and a data section, to which a check element generated from the contents of the message is appended. The data section of the message is then signed and/or encrypted so as to permit the receiver to reliably identify the identity of the sender. Use of the check element additionally permits confirmation that the message contents have not been unintendedly modified or corrupted and that the message has been decrypted using the correct decryption key.

FOR OFFICIAL USE ONLY